CLAIMS

1. A client for connecting a mobile host to a remote network through an access network with a single user password, where the access network may be independent of the remote network in terms of no protocol conversation between authentication servers in the access network and the remote network, respectively, and a virtual single account (VSA) has been set up for a user to connect to the access network and then to the remote network, the client comprising machine readable instructions stored in a memory medium, which when executed by a processor:

generate a VSA password and decryption key from the single password received from the user;

decrypt at least one of a local access network authentication credential and a remote access authentication credential;

initiate a local access network connection; and

initiate a remote network access connection.

2. The client recited in Claim 1, wherein the machine-readable instructions, which when executed by the processor, initiate a VSA configuration update process with a VSA server.

3. The client recited in Claim 2, wherein the machine-readable instructions, which when executed by the processor, initiate the VSA configuration update process by:

constructing a VSA information update request message;

sending the VSA information update request message to the VSA server; and

receiving a VSA information update response message from the VSA server.

4. The client recited in Claim 3, wherein the step of decrypting the remote network authentication credential prior to initiating the remote network access connection is authorized by an instruction for the mobile host in the VSA information update request message.

5. The client recited in Claim 1, wherein the machine-readable instructions, which when executed by the processor, select a local access network from a current VSA access record stored in the memory medium.

6. The client recited in Claim 1, wherein the machine-readable instructions, which when executed by the processor, generate the decryption key in response to a random sequence received from the user.

7. The client recited in Claim 1, wherein the machine-readable instructions, which when executed by the processor, generate the VSA password using the expression: VSA password = hash(VSA username || common password || VSA server || remote network ID), wherein the VSA username identifies the user to a VSA server, the common password is the single password from the user, and the remote network ID identifies the remote network serving as a home network for the mobile host.

8. The client recited in Claim 3, wherein the machine-readable instructions, which when executed by the processor, generate the VSA update

request message "Q" from the expression: Q = VSA username || X || E_{K1} (Synchronization time || Request content), where X is a random sequence; and K1 is an encryption key calculated from hash (hash (VSA password) || X).

9. The client recited in Claim 8, wherein the machine-readable instructions, which when executed by the processor, are responsive to the VSA information update response message "A" derived from the expression: A = Response Code || Y || E_{K2} (Synchronization time || Response content), wherein Y is a random sequence, and K2 is an encryption key calculated from hash (hash (VSA password) || Y).

10. The client recited in Claim 1, wherein the machine-readable instructions, which when executed by the processor, select local access parameters and remote access parameters from a VSA access record stored in the memory medium.

11. A system for connecting a mobile host to a remote network through an access network with a single password, where the access network may be independent of the remote network in terms of no protocol conversation between authentication servers in the access network and the remote network, respectively, and a virtual single account (VSA) has been set up for a user to connect to the access network and then to the remote network, comprising:

a VSA server deployed in the remote network, the VSA server including machine readable instructions stored in a memory medium, which when executed by a processor:

send a VSA information update response message to the mobile host in response to receiving a VSA information update request message from the mobile host;

verify an authentication credential for the remote network received from the mobile host; and

authorize a remote gateway in the remote network to connect the mobile host to the remote network.

12. The system recited in Claim 11, wherein the VSA server includes machine readable instructions stored in the memory medium, which when executed by the processor generate the VSA information update response message "A" from the expression: A = Response Code || Y || E_{K2} (Synchronization time || Response content), wherein Y is a random sequence, and K2 is an encryption key calculated from hash (hash (VSA password) || Y), in response to the VSA information update request message "Q" from the expression: Q = VSA username || X || E_{K1} (Synchronization time || Request content), where X is a random sequence; and K1 is an encryption key calculated from hash (hash (VSA password) || X).

13. The system recited in Claim 11, wherein the VSA server contains a plurality of VSA management records, each management record including a user's VSA authentication credential.

14. The system recited in Claim 11, wherein the VSA server maintains access information for at least one local access network and at least one remote network.

15. The system recited in Claim 14, wherein the access information includes client information for mobile hosts, and management information for at least one additional VSA server.